Amendments to the Specification:

Please replace paragraph (0003) with the following amended paragraph:

(0003) Computer networks and systems have become indispensable tools for modern business. Modern enterprises use such networks for communications and for storage. The information and data stored on the network of a business enterprise is often a highly valuable asset. Modern enterprises use numerous tools to keep outsiders, intruders, and unauthorized personnel from accessing valuable information stored on the network. These tools include firewalls, intrusion detection systems, and packet sniffer devices. However, once an intruder has gained access to sensitive content, there is no network device that can prevent the electronic transmission of the content from the network to outside the network. Similarly, there is no network device that can ~~analyse~~ analyze the data leaving the network to monitor for policy violations, and make it possible to track down information ~~looks~~ leaks. What is needed is a comprehensive system to capture, store, and ~~analyse~~ analyze all data communicated using the enterprises network.

Please replace paragraph (0019) with the following amended paragraph:

(0019) FIG. 1 illustrates a simple prior art configuration of a local area network (LAN) 10 connected to the Internet 12. Connected to the LAN ~~102~~ 10 are various components, such as servers 14, clients 16, and switch 18. There

are numerous other known networking components and computing devices that can be connected to the LAN 10. The LAN 10 can be implemented using various wireline or wireless technologies, such as Ethernet and 802.11b. The LAN 10 may be much more complex than the simplified diagram in FIG. 1, and may be connected to other LANs as well.

Please replace paragraph (0020) with the following amended paragraph:

(0020) In FIG. 1, the LAN 10 is connected to the Internet 12 via a router 20. This router 20 can be used to implement a firewall, which are widely used to give users of the LAN 10 secure access to the Internet 12 as well as to separate a company's public Web server (can be one of the servers 14) from its internal network, i.e., LAN 10. In one embodiment, any data leaving the LAN 10 towards the Internet 12 must pass through the router ~~12~~ 20. However, there the router 20 merely forwards packets to the Internet 12. The router 20 cannot capture, ~~analyse~~ analyze, and ~~searchably~~ store, in a searchable manner, the content contained in the forwarded packets.

Please replace paragraph (0021) with the following amended paragraph:

(0021) One embodiment of the present invention is now illustrated with reference to FIG. 2. FIG. 2 shows the same simplified configuration of connecting the LAN 10 to the Internet 12 via the router 20. However, in FIG. 2, the router 20 is also connected to a capture system 22. In one embodiment,

the router ~~12~~ 20 splits the outgoing data stream, and forwards one copy to the Internet 12 and the other copy to the capture system 22.

Please replace paragraph (0022) with the following amended paragraph:

(0022) There are various other possible configurations. For example, the router 12 can also forward a copy of all incoming data to the capture system 22 as well. Furthermore, the capture system 22 can be configured sequentially in front of, or behind the router 20, however this makes the capture system 22 a critical component in connecting to the Internet 12. In systems where a router ~~12~~ 20 is not used at all, the capture system can be interposed directly between the LAN 10 and the Internet 12. In one embodiment, the capture system 22 has a user interface accessible from a LAN-attached device, such as a client 16.

Please replace paragraph (0027) with the following amended paragraph:

(0027) In one embodiment, the reassembler 36 begins a new flow upon the observation of a starting packet defined by the data transfer protocol. For a TCP/IP embodiment, the starting packet is generally referred to as the "SYN" packet. The flow can terminate upon observation of a finishing packet, e.g., a "Reset" or "FIN" packet in TCP/IP. If now finishing packet is observed by the reassembler 36 within some time constraint, it can terminate

the flow via a timeout mechanism.~~.~~ In an embodiment using the TPC protocol, a TCP flow contains an ordered sequence of packets that can be assembled into a contiguous data stream by the ~~reassembler~~ reassembler 36. Thus, in one embodiment, a flow is an ordered data stream of a single communication between a source and a destination.

Please replace paragraph (0030) with the following amended paragraph:

(0030) The ~~flown~~ flow assembled by the ~~reassembler~~ reassembler 36 can then be provided to a protocol demultiplexer (demux) 38. In one embodiment, the protocol demux 38 sorts assembled flows using the TCP Ports. This can include performing a speculative classification of the flow contents based on the association of well-known port numbers with specified protocols. For example, Web Hyper Text Transfer Protocol (HTTP) packets--i.e., Web traffic--are typically associated with port 80, File Transfer Protocol (FTP) packets with port 20, Kerberos authentication packets with port 88, and so on. Thus in one embodiment, the protocol demux 38 separates all the different protocols in one flow.

Please replace paragraph (0040) with the following amended paragraph:

(0040) In several embodiments, the capture system 22 has been described above as a stand-alone device. However, the capture system of the present invention can be implemented on any appliance capable of

capturing and ~~analysing~~ analyzing data from a network. For example, the capture system 22 described above could be implemented on one or more of the servers 14 or clients 16 shown in Figure 1. The capture system 22 can interface with the network 10 in any number of ways, including wirelessly.